ARTICLE VI
FRAUD CONTROL, NETWORK SECURITY AND LAW ENFORCEMENT

6.0 Fraud Control, Network Security and Law Enforcement.

6.1 Protection of Service and Property.

6.1.1 The Parties will exercise due care to prevent harm or damage to their respective employees, agents or customers, or their property. The Parties' employees, agents, or representatives agree to take reasonable and prudent steps to ensure the adequate protection of their respective property and services. In recognition of its obligation under this Article, SBC-AMERITECH agrees to take the following reasonable and prudent steps, including but not limited to:

6.1.2 Restricting access to AT&T equipment, support equipment, systems, tools and data, or spaces which contain or house AT&T equipment to the extent SBC-AMERITECH provides this protection to its own facilities. SBC-AMERITECH will provide access to AT&T employees and its agents based on AT&T providing a list of authorized personnel. AT&T employees and authorized agents must display identification required by SBC-AMERITECH.

6.1.3 SBC-AMERITECH will follow mutually agreed upon notification procedures in the event it becomes necessary for an SBC-AMERITECH employee to enter into the exclusive AT&T collocated space.

6.1.4 Each Party will comply at all times with the other Party's, i.e., the Landlord's, security and safety procedures and requirements, including but not limited to, sign in and identification requirements while in spaces which house or contain the other Party's equipment or equipment enclosures.

6.1.5 Allowing AT&T to inspect or observe spaces which house or contain AT&T equipment or equipment enclosures after such time as SBC-AMERITECH has turned over the collocation area to AT&T and to furnish AT&T with all keys, entry codes, lock combinations, or other materials or information which may be needed to gain entry into any secured AT&T space.

6.1.6 Providing card access, coded locks or keyed locks providing security to the exclusive AT&T collocated space that is unique to that space.

6.1.7 Ensuring that the area that houses AT&T's equipment is adequately secured to prevent unauthorized entry to the same level as SBC-AMERITECH provides to itself.

6.1.8 Limiting the keys used in SBC-AMERITECH's keying systems for cages which contain or house AT&T equipment or equipment enclosures to SBC-AMERITECH's employees or required safety personnel (in compliance with governing building or fire codes) for required access only. Any access required other than emergency access will be coordinated with AT&T to allow escort opportunity. SBC-AMERITECH will change locks at AT&T's request. The expense will be borne by SBC-AMERITECH where a security breach is known or suspected and the breach is caused by SBC-AMERITECH.

6.1.9 Installing security studs in the hinge plates of doors having exposed hinges with removable pins that lead to spaces or equipment enclosures which house or contain AT&T equipment, provided AT&T has requested the installation of such security studs and has agreed to pay the full expense for such installation.

6.1.10 Controlling unauthorized access from passenger and freight elevators by continuous surveillance or by installing security partitions, security grills, locked gates or doors between elevator lobbies and spaces which contain or house AT&T equipment or equipment enclosures.

6.1.11 Providing notification to designated AT&T personnel to report any actual or attempted security breach involving AT&T's equipment or equipment enclosures as soon as reasonably practicable after SBC-AMERITECH has become aware of such actual or attempted security breach.

6.1.12 Each Party agrees to provide to the other Party its back-up and recovery plan for review and reasonable acceptance by the other Party to be used in the event of a security system failure or emergency.

6.1.13 In the event that **Article XII** addresses any matter also covered by this Article, the provisions of **Article XII** prevail.

6.2 Data and System Protection.

6.2.1 Joint Security Requirements.

6.2.1.1 Both Parties will maintain accurate and auditable records that monitor user authentication and machine integrity and confidentiality (e.g., password assignment and aging, chronological logs configured, system accounting data, etc.).

6.2.1.2 Both Parties shall maintain accurate and complete records detailing the individual data connections and systems to which they have granted the other Party access or interface privileges. These records will include, but are not limited to, user ID assignment, user request records, system configuration, and time limits of user access or system interfaces. These records should be kept until the termination of

this Agreement, or the termination of the requested access by the identified individual. Either Party may initiate a compliance review of the connection records to verify that only the agreed to connections are in place and that the connection records are accurate.

6.2.1.3 Each Party shall notify the other party immediately upon termination of employment of an individual user with approved access to the other Party's network.

6.2.1.4 Both Parties shall use an industry standard virus detection software program at all times. The Parties shall immediately advise each other by telephone upon actual knowledge that a virus or other malicious code has been transmitted to the other Party.

6.2.1.5 All physical access to equipment and services required to transmit data will be in secured locations. Verification of authorization will be required for access to all such secured locations. A secured location is where walls and doors are constructed and arranged to serve as barriers and to provide uniform protection for all equipment used in the data connections that are made as a result of the user's access to either the AT&T or SBC-AMERITECH network. At a minimum, this shall include: access doors equipped with card reader control or an equivalent authentication procedure and/or device, and egress doors which generate a real-time alarm when opened and which are equipped with tamper resistant and panic hardware as required to meet building and safety standards.

6.2.1.6 Both Parties shall maintain accurate and complete records on the card access system or lock and key administration to the rooms housing the equipment utilized to make the connection(s) to the other Party's network. These records will include management of card or key issue, activation, or distribution and deactivation.

6.2.2 Additional Responsibilities of Both Parties.

6.2.2.1 Modem/DSU Maintenance And Use Policy. To the extent the access provided hereunder involves the support and maintenance of AT&T equipment on SBC-AMERITECH's premises, such maintenance will be provided under terms agreed to by the Parties.

6.2.2.2 Monitoring. Each Party will monitor its own network relating to any user's access to the Party's networks, processing systems, and applications. This information may be collected, retained, and analyzed to identify potential security risks without notice. This information may include, but is not limited to, trace files, statistics, network addresses, and the actual data or screens accessed or transferred.

6.2.2.3 Each Party shall notify the other Party's security organization immediately upon initial discovery of actual or suspected unauthorized access to, misuse

of, or other "at risk" conditions regarding the identified data facilities or information. Each Party shall provide a specified point of contact. If either Party suspects unauthorized or inappropriate access, the Parties shall work together to isolate and resolve the problem.

6.2.2.4 In the event that one Party identifies inconsistencies or lapses in the other Party's adherence to the security provisions described herein, or a discrepancy is found, documented and delivered to the non-complying Party, a corrective action plan to address the identified vulnerabilities must be provided by the non-complying Party within thirty (30) calendar days of the date of the identified inconsistency. The corrective action plan must identify what will be done, the Party accountable/responsible, and the proposed compliance date. The non-complying Party must provide periodic status reports to the other Party's security organization on the implementation of the corrective action plan in order to track the work to completion.

6.2.2.5 In the event there are technological constraints or situations where either Party's corporate security requirements cannot be met, the Parties will institute mutually agreed upon alternative security controls and safeguards to mitigate risks.

6.2.2.6 All network-related problems will be managed to resolution by the respective organizations, AT&T or SBC-AMERITECH, as appropriate to the ownership of a failed component. As necessary, AT&T and SBC-AMERITECH will work together to resolve problems where the responsibility of either Party is not easily identified.

6.2.3 Information Security Policies And Guidelines For Access To Computers, Networks and Information By Non-Employee Personnel.

6.2.3.1 Information security policies and guidelines are designed to protect the integrity, confidentiality and availability of computer, networks and information resources. This summary provides a convenient reference for individuals who are not employees of the Party that provides the computer, network or information, but have authorized access to that Party's systems, networks or information. Questions should be referred to AT&T or SBC-AMERITECH, respectively, as the providers of the computer, network or information in question.

6.2.3.2 It is each Party's responsibility to notify its employees, contractors and vendors who will have access to the other Party's network, on the proper security responsibilities identified within this Article. Adherence to these policies is a requirement for continued access to the other Party's systems, networks or information. Exceptions to the policies must be requested in writing and approved by the other Party's information security organization.

6.2.4 General Policies.

6.2.4.1 Each Party's resources are for approved business purposes only.

6.2.4.2 Each Party may exercise at any time its right to inspect, record, and/or remove all information contained in its systems, and take appropriate action should unauthorized or improper usage be discovered.

6.2.4.3 Individuals will only be given access to resources that they are authorized to receive, and which they need to perform their job duties. Users must not attempt to access resources for which they are not authorized.

6.2.4.4 Authorized users must not develop, copy or use any program or code that circumvents or bypasses system security or privilege mechanism or distorts accountability or audit mechanisms.

6.2.4.5 Actual or suspected unauthorized access events must be reported immediately to each Party's security organization or to an alternate contact identified by that Party. Each Party shall provide its respective security contact information to the other.

6.2.5 User Identification.

6.2.5.1 Access to each Party's corporate resources will be based on identifying and authenticating individual users in order to maintain clear and personal accountability for each user's actions.

6.2.5.2 User identification shall be accomplished by the assignment of a unique, permanent userid, and each userid shall have an associated identification number for security purposes.

6.2.5.3 Userids will be revalidated pursuant to each Party's corporate policies.

6.2.6 User Authentication.

6.2.6.1 Users will usually be authenticated by use of a password. Strong authentication methods (e.g. one-time passwords, digital signatures, etc.) may be required in the future.

6.2.6.2 Passwords must not be stored in script files.

6.2.6.3 Passwords must be entered by the user in real time.

6.2.6.4 Passwords must be at least six to eight (6-8) characters in length, not blank or a repeat of the userid; contain at least one letter, and at least one number or special character must be in a position other than the first or last one. This format will ensure that the password is hard to guess. Most systems are capable of being configured to automatically enforce these requirements. Where a system does not mechanically require this format, the users must manually follow the format.

6.2.6.5 Systems will require users to change their passwords regularly (usually every thirty-one (31) days).

6.2.6.6 Systems are to be configured to prevent users from reusing the same password for six (6) changes/months.

6.2.6.7 Personal passwords must not be shared. A user who has shared his password is responsible for any use made of the password.

6.2.7 Access and Session Control.

6.2.7.1 Destination restrictions will be enforced at remote access facilities used for access to OSS Interfaces. These connections must be approved by each Party's corporate security organization.

6.2.7.2 Terminals or other input devices must not be left unattended while they may be used for system access. Upon completion of each work session, terminals or workstations must be properly logged off.

6.2.8 User Authorization.

6.2.8.1 On the destination system, users are granted access to specific resources (e.g. databases, files, transactions, etc.). These permissions will usually be defined for an individual user (or user group) when a userid is approved for access to the system.

6.2.9 Software and Data Integrity.

6.2.9.1 Each Party shall use a comparable degree of care to protect the other Party's software and data from unauthorized access, additions, changes and deletions as it uses to protect its own similar software and data. This may be accomplished by physical security at the work location and by access control software on the workstation.

6.2.9.2 Untrusted software or data shall be scanned for viruses before use on a Party's corporate facilities that can be accessed through the direct connection or dial up access to OSS interfaces.

6.2.9.3 Unauthorized use of copyrighted software is prohibited on each Party's corporate systems that can be access through the direct connection or dial up access to OSS Interfaces.

6.2.9.4 Proprietary software or information (whether electronic or paper) of a Party shall not be given by the other Party to unauthorized individuals. When it is no longer needed, each Party's proprietary software or information shall be returned by the other Party or disposed of securely. Paper copies shall be shredded. Electronic copies shall be overwritten or degaussed.

6.2.10 Monitoring and Audit.

6.2.10.1 To deter unauthorized access events, a warning or no-trespassing message will be displayed at the point of initial entry (i.e., network entry or applications with direct entry points). Each Party should have several approved versions of this message. Users should expect to see a warning message similar to this one:

"This is a (SBC-AMERITECH or AT&T) system restricted to Company official business and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use, or modification being used for criminal prosecution."

6.2.10.2 After successful authentication, each session will display the last logon date/time and the number of unsuccessful logon attempts. The user is responsible for reporting discrepancies.

6.3 Revenue Protection.

6.3.1 SBC-AMERITECH will make available to AT&T all present and future fraud prevention or revenue protection features, including prevention, detection, or control functionality to the same extent that SBC-AMERITECH provides such protection to itself. These features include, but are not limited to, screening codes and call blocking of international, 900 and 976 numbers. These features may include: (i) disallowance of call forwarding to international locations, (ii) coin originating ANI II digits, (iii) dial tone re-origination patches, (iv) terminating blocking of 800 and (v) 900/976 blocking.

6.3.2 SBC-AMERITECH will provide to AT&T the same procedures to detect and correct the accidental or malicious alteration of software underlying Network Elements or their subtending operational support systems by unauthorized third parties in the same manner it does so for itself.

6.3.3 SBC-AMERITECH will make a reasonable effort to protect and correct against unauthorized physical attachment, e.g. clip-on fraud, to loop facilities from the Main Distribution Frame up to and including the Network Interface Device.

6.3.4 The Parties shall work cooperatively to minimize fraud associated with third-number billed calls, calling card calls, and any other services related to this Agreement.

6.3.4.1 In the event of fraud associated with an AT&T End User's account, the parties agree that liability should be determined based on the facts related to the incident of fraud. SBC-AMERITECH shall not be liable for any fraud associated with an AT&T end user's account unless such fraud is determined to have been committed by an employee or other person under the control of SBC-AMERITECH.

Alternatively Billed Service ("ABS") is a service that allows End Users to bill calls to account(s) that might not be associated with the originating line. There are three types of ABS calls: calling card, collect, and third number billed calls.

6.3.4.2 SBC-AMERITECH shall use the Sleuth system to determine suspected occurrences of ABS-related fraud for AT&T customers, using the same criteria SBC-AMERITECH uses to monitor fraud on its own accounts. As used herein, "Sleuth" shall mean "Sleuth system or comparable fraud detection system".

6.3.4.2.1 SBC-AMERITECH will provide notification messages to AT&T on suspected occurrences of ABS-related fraud on AT&T accounts stored in the applicable LIDB. SBC-AMERITECH will provide these fraud notification messages ("alerts") to AT&T within two (2) hours of the Sleuth alert being generated. Subsequent to AT&T's investigation of the Sleuth alert, AT&T's Fraud Center will notify SBC-AMERITECH of any action that needs to be taken. SBC-AMERITECH will complete such action as requested by AT&T within two (2) hours of AT&T's request.

6.3.4.2.2 AT&T understands that Sleuth alerts only identify potential occurrences of fraud. AT&T understands and agrees that it will need to perform its own investigations to determine whether a fraud situation actually exists. AT&T understands and agrees that it will also need to determine what, if any, action should be taken as a result of a Sleuth alert.

6.3.4.2.3 The Parties will provide contact names and numbers to each other for the exchange of Sleuth alert notification information twenty-four (24) hours per day seven (7) days per week.

6.3.4.2.4 For each alert notification provided to AT&T, AT&T may request a corresponding thirty-day (30-day) historical report of ABS-related query processing. AT&T may request up to three reports per alert.

6.3.4.2.5 ABS-related alerts are provided to AT&T at no additional charge.

6.3.4.3 Within six (6) months of approval of this Agreement by the Commission, SBC-AMERITECH will provide AT&T with a direct, near real time, electronic transmission of LIDB requests for Alternatively Billed Services (Collect and/or Billed to Third Party calls billed to AT&T customers) in the same manner SBC-AMERITECH does so for itself.

6.3.5 The Parties agree that AT&T reserves the right to negotiate, as needed, the rates, terms and conditions of a 1+ IntraLATA toll fraud service provided by SBC-AMERITECH.

6.4 Law Enforcement Interface.

6.4.1 SBC-AMERITECH will provide AT&T with a SPOC with whom to interface on a twenty-four (24) hour, seven (7) day a week basis for situations involving immediate threat to life or at the request of law enforcement officials. Court orders authorizing surveillance of AT&T customers provisioned on SBC-AMERITECH facilities (AT&T Local and ALS Type II, as hereinafter defined) shall be served on both AT&T and SBC-AMERITECH. SBC-AMERITECH shall provide law enforcement with all necessary assistance, including plant information and local loop access, to facilitate implementation of such court orders. Once AT&T implements CALEA solutions in its switches, AT&T will assume full responsibility for the implementation of court-ordered surveillance on ALS Type II customers.

6.4.1.1 As used in this Article, the term ALS Type II shall mean customers connected to the AT&T network through SBC-AMERITECH-owned facilities. ALS Type II customers are located in a building which is connected to an SBC-AMERITECH Central Office by an SBC-AMERITECH-owned cable using customer's premise equipment connected to that cable. At the SBC-AMERITECH Central Office utilizing collocation arrangements, ALS Type II customer's circuit(s) are connected to an AT&T fiber-optic facility which transports traffic to and from an AT&T Central Office.

6.4.2 When the end-user to be tapped, traced, etc. is an AT&T Local or ALS Type II customer provisioned on SBC-AMERITECH facilities, SBC-AMERITECH shall advise the requesting law enforcement agency to name both AT&T and SBC-AMERITECH in the court order and serve both carriers. SBC-AMERITECH shall adhere to all terms of an applicable court order and, unless prohibited by the terms of such applicable court order, notify AT&T directly of the law enforcement agency request within one (1) business day of receiving the request. SBC-AMERITECH shall provide law enforcement with all necessary assistance, including plant information and access to the local loop, to facilitate implementation of such court orders. Once AT&T implements CALEA solutions in its switches, AT&T will assume full responsibility for the implementation of court-ordered surveillance on ALS Type II customers.

6.4.3 Each Party shall bill the appropriate law enforcement agency for these services under its customary practices. Where the law enforcement agency will not reimburse the Party for its compliance with a court order or other request for information, each Party shall be responsible for its own costs associated with compliance or assisting the other Party to comply.

6.4.4 SBC-AMERITECH and AT&T shall reasonably cooperate with the other Party in handling law enforcement requests as follows:

6.4.4.1 Intercept Devices. Should either Party receive a court order authorizing surveillance on the other Party's End User, the Party in receipt shall refer such order to the Party that serves the End User. Should a court order pertain to an AT&T Local customer (trap & trace, pen register or wiretap) or an ALS Type II customer (pen register or wiretap), the Party in receipt will request the issuing authority to amend the order, naming both Parties, and serve both Parties concurrently. SBC-AMERITECH shall provide law enforcement with all necessary assistance, including plant information and local loop access, to facilitate implementation of court orders pertaining to pen registers or wiretaps. Additionally, SBC-AMERITECH shall provision on its equipment trap & trace orders pertaining to AT&T Local customers. As specified in **Section 6.4.3**, above SBC-AMERITECH may bill the appropriate law enforcement agency for these services under its customary practices. Once AT&T implements CALEA solutions in its switches, AT&T will assume full responsibility for the implementation of court-ordered surveillance on ALS Type II customers.

6.4.4.2 Subpoenas. Should either Party receive a subpoena for subscriber information or billing records concerning the other Party's End User, it shall refer the subpoena back to the issuing authority. The referral shall indicate that the other Party is the responsible company, unless the subpoena requests records for a period of time during which the receiving Party was the End User's service provider, in which case that Party will respond to any valid request. Should the subpoena demand AMA records (call dump) for an AT&T Local customer, the Party in receipt will request the issuing authority to amend the order, naming both Parties, and serve both Parties concurrently. SBC-AMERITECH shall provide the issuing authority with the requested data. As specified in **Section 6.4.3**, above SBC-AMERITECH may bill the appropriate law enforcement agency for these services under its customary practices.

6.4.4.3 Emergencies. If a Party receives a request from a law enforcement agency for a temporary number change, temporary disconnect, or one-way denial of outbound calls by the receiving Party's switch for an End User of the other Party, that Receiving Party will comply with a valid emergency request. However, neither Party shall be held liable for any claims or Losses arising from compliance with such requests on behalf of the other Party's End User and the Party serving such End User agrees to indemnify and hold the other Party harmless against any and all such claims or Losses.

6.4.5 Annoyance Calls. SBC-AMERITECH agrees to work cooperatively and jointly with AT&T in investigating annoyance/harassing calls to the AT&T customer where SBC-AMERITECH's cooperation, services, unbundled network elements (including operational support systems), facilities or information are needed to resolve the annoyance/harassing call(s) to the AT&T customer. The SBC-AMERITECH Annoyance Call Bureau will handle requests received from AT&T personnel on behalf of AT&T customers. SBC-AMERITECH will provide service to AT&T customers on annoyance/harassing calls that is at parity with the level of service SBC-AMERITECH provides its own customers.

6.4.6 CALEA. Each Party represents and warrants that any equipment, facilities or services provided to the other Party under this Agreement comply with the Communications Assistance for Law Enforcement Act of 1994 **("CALEA")** as amended, including any final orders of the FCC, or final regulations promulgated by the Federal Bureau of Investigation, Department of Justice, or any other federal agency pursuant to CALEA.

6.4.6.1 The Parties agree to work jointly, cooperatively and in good faith to allow each Party to comply with CALEA.

6.4.6.2 Unless otherwise specified, each Party shall bear its own cost of complying with CALEA.

6.4.7 Soft Dial Tone. To the extent required by law and subject to such additional conditions as the Parties may require, SBC-AMERITECH shall provide soft dial tone to AT&T for the use of its customers.